

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION**

Lane Gay, on behalf of himself and all others similarly situated, Plaintiff, v. Mortgage Contracting Services, LLC, Defendant.	Case No.: 4:24-cv-00217-SDJ JURY TRIAL DEMANDED
---	---

AMENDED CLASS ACTION COMPLAINT

Plaintiff, Lane Gay, through his attorneys, brings this Amended Class Action Complaint against the Defendant, Mortgage Contracting Services, LLC (“MCS” or “Defendant”), alleging as follows:

INTRODUCTION

1. On or around February 22, 2024, Mortgage Contracting Services, announced it had lost control over its computer network and the highly sensitive private information stored on the computer network in a data breach by cybercriminals (“Data Breach”).¹ On information and belief, the Data Breach has impacted at least 1,143 of MCS’s current and former employees and customers.²

2. Due the deliberately obfuscating language of Defendant’s Breach Notice, it is unclear when the unauthorized party first gained access to Defendant’s network and how long

¹ Data Breach Notice, New Hampshire Department of Justice, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.doj.nh.gov/consumer/security-breaches/documents/mortgage-contracting-services-20240222.pdf (last visited 03/06/24).

² Data Security Breach Reports, Attorney General of Texas, <https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage> (last visited 03/10/24).

cybercriminals had unfettered excess to Plaintiff's and the Class's sensitive and private information. However, upon information and belief, the breach occurred between December 9, 2023 and December 13, 2023.³

3. Following discovery of the Breach, Defendant conducted an internal investigation which revealed that cybercriminals gained unauthorized access to former and current employees' and customers' personally identifiable information ("PII"), including but not limited to their names and Social Security numbers.

4. On or around February 22, 2024, almost three months after the breach occurred, Defendant finally began notifying victims about the breach.⁴ An example Breach Notice has been attached as Exhibit A (the "Breach Notice"). During this time, Plaintiff and Class Members were unaware that their PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm.

5. MCS failed to reasonably secure, monitor, and maintain the PII provided to it by its former and current customers and employees. Upon information and belief, the Data Breach resulted in the likely unauthorized access, download, exfiltration, and misuse of the PII by the cyber criminals who targeted that information through their wrongdoing.

6. Defendant's Breach Notice obfuscated the nature of the breach and the threat it posed—refusing to tell its victims how many people were impacted, how the breach happened, or why MCS delayed notifying its victims that hackers had gained access to highly sensitive PII.

7. Defendant's failure to timely detect and report the Data Breach made its customers vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

³ *Id.*

⁴ *Id.*

8. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

9. In failing to adequately protect customers' and employees' information, adequately notify them about the breach, and obfuscating the nature of the breach, Defendant violated state law and harmed at least 1,143 of its former and current customers.

10. Plaintiff and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiff and the Class trusted Defendant with their PII. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

11. Plaintiff is a former MCS employee and a Data Breach victim.

12. Accordingly, Plaintiff, on behalf of himself and on behalf of a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

PARTIES

13. Plaintiff, Lane Gay, is a natural person and citizen of Louisiana, residing in Ruston, Louisiana, where he intends to remain. Mr. Gay is a Data Breach victim.

14. Defendant, MCS, is a Delaware Limited Liability Company with its principal place of business at 350 Highland Drive Suite 100, Lewisville, Texas 75067.

15. Defendant's sole member is Lender MCS Acquisition Corporation. Lender MCS Acquisition Corporation is incorporated in Delaware with its principal place of business at 350 Highland Drive Suite 100, Lewisville, Texas 75067. Thus, Lender MCS Acquisition Corporation is a citizen of Delaware and Texas.

16. Plaintiff is a citizen of Louisiana and Defendant, MCS, is a citizen of Delaware and Texas.

JURISDICTION & VENUE

17. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class; Plaintiff and Defendant are citizens of different states.

18. MCS is a Delaware LLC and maintains its principal place of business at 350 Highland Drive Suite 100, Lewisville, Texas 75067. MCS is thus a Delaware and Texas citizen.

19. Lender MCS Acquisition Corporation is incorporated in Delaware with its principal place of business at 350 Highland Drive Suite 100, Lewisville, Texas 75067. Lender MCS Acquisition Corporation is thus a Delaware and Texas citizen.

20. This Court has personal jurisdiction over MCS because it is a citizen of this District and maintains its headquarters and principal place of business in the Sherman Division of the Eastern District of Texas.

21. Venue is proper because MCS maintains its headquarters and principal place of business in the Sherman Division of the Eastern District of Texas.

BACKGROUND FACTS

Mortgage Contracting Services

22. MCS is a nationwide property services provider based in Texas. Founded in 1986, MCS evolved into one of the premier default and property preservation providers for the mortgage industry, building relationships with many of the largest financial institutions across the

country.⁵ MCS boasts a staggering annual revenue of over 91 million dollars.⁶

23. On information and belief, MCS accumulates highly sensitive PII Information of its customers.

24. On information and belief, MCS maintains former and current customers' and employees' PII for years after the customer's relationship with Defendant is terminated.

25. According to its website, MCS is "committed to treating and using personal information about you responsibly" and that it "employs technical safeguards, as well as internal policies, procedures, and controls, to protect the information from unauthorized access or disclosure."⁷

26. MCS understood the need to protect its employees' data and prioritize its data security. However, despite recognizing its duty to do so, on information and belief, MCS has not in fact implemented reasonably cybersecurity safeguards or policies to protect its employees' PII or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, MCS leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to former and current employees' PII.

MCS Fails to Safeguard Customer PII

27. Plaintiff is a former employee of MCS.

28. As a condition of employment with MCS, Plaintiff provided Defendant with his PII. As a condition of employment with MCS, Defendant requires its employees to disclose PII including but not limited to, their name and Social Security number. Defendant used that PII to facilitate its employment of Plaintiff, including payroll, and required Plaintiff to provide that PII

⁵ About MCS, MCS, <https://mcs360.com/about-mcs/> (last visited March 6, 2024).

⁶ MCS, Zoominfo, <https://www.zoominfo.com/c/mortgage-contracting-services-llc/354433113> (last visited March 6, 2024).

⁷ Privacy Policy, MCS, <https://mcs360.com/privacy-policy/> (last visited March 6, 2024).

to obtain employment and payment for that employment.

29. Similarly, as a condition of receiving mortgage services from MCS, Defendant requires its customers to provide it with their PI, including but not limited to name and Social Security number.

30. In collecting and maintaining customers' and employees' PII, MCS implicitly agrees it will safeguard the data using reasonable means according to its internal policies, as well as state and federal law.

31. According to the Breach Notice, MCS claims to have experienced "an incident that that involved unauthorized access to certain company computer systems" on December 9, 2023. Following an internal investigation MCS admitted that "an unauthorized actor acquired certain files stored on its computer servers" as a result of the Breach.⁸ In other words, Defendant's investigation revealed that its network had been hacked by cybercriminals and that Defendant's inadequate cyber and data security systems and measures allowed those responsible for the cyberattack to obtain files containing a treasure trove of thousands of MCS former and current customers' and employees' PII.

32. Despite its duties and alleged commitments to safeguard PII, MCS does not follow industry standard practices in securing former and current customers' and employees' PII, as evidenced by the Data Breach.

33. In response to the Data Breach, Defendant contends that it has "implemented additional safeguards and technical security measures to enhance the security of our network." Ex.

A. Although Defendant fails to expand on what these alleged "safeguards and technical security

⁸ Data Breach Notice, New Hampshire Department of Justice, chrome-extension://efaidnbmninnibpcjpcglclefindmkaj/https://www.doj.nh.gov/consumer/security-breaches/documents/mortgage-contracting-services-20240222.pdf (last visited 03/06/24).

measures” are, such steps should have been in place before the Data Breach.

34. Through its Breach Notice, MCS recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to sign up for identity monitoring services including credit monitoring, fraud consultation, and identity theft restoration. Ex. A.

35. MCS offered Data Breach victims two years of complimentary identity monitoring services, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves PII that cannot be changed, such as Social Security numbers. Further, the breach exposed employees’ nonpublic, highly private information, a disturbing harm in and of itself.

36. Even with complimentary credit monitoring services, the risk of identity theft and unauthorized use of Plaintiff’s and Class Members’ PII is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

37. Cybercriminals need not harvest a person’s Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff’s and the Class’s PII. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create “Fullz” packages, which can then be used to commit fraudulent account activity on Plaintiff’s and the Class’s financial accounts.

38. Through its inadequate security practices, Defendant exposed Plaintiff’s and the Class’s PII for theft and sale on the dark web.

39. On information and belief, MCS failed to adequately train its IT and data security employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its former and current customers’ PII. Defendant’s negligence is

evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII.

Plaintiff's Experience

40. Plaintiff is a former MCS employee.

41. As a condition of employment with MCS, Mr. Gay was required to provide his PII to Defendant and trusted that the company would use reasonable measures to protect it according to MCS' internal policies and state law.

42. Mr. Gay received a Breach Notice from MCS on or around March 3, 2024, stating that his PII was exposed during the Data Breach.

43. Due to MCS's obfuscating language, it was unclear to Plaintiff how and when the Data Breach occurred, and how long cybercriminals had unfettered access to his PII. Ex. A.

44. MCS deprived Plaintiff of the earliest opportunity to guard his PII against the Data Breach's effects by failing to immediately and promptly notify him about it.

45. As a result of the Data Breach and the recommendation of Defendant's Notice Plaintiff has spent several hours of his uncompensated time dealing with the consequences of the Data Breach, which includes uncompensated time spent verifying the legitimacy of the Notice of Data Breach, and self-monitoring his information to ensure no fraudulent activity has occurred. This uncompensated time has been lost forever and cannot be recaptured.

46. Mr. Gay fears for his personal financial security and uncertainty over what PII exposed in the Data Breach. Mr. Gay has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

47. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's PII for

theft by cybercriminals and sale on the dark web.

48. Plaintiff suffered actual injury from the exposure of his PII—which violates his rights to privacy.

49. Plaintiff has suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

50. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties and possibly criminals.

51. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

52. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

53. The ramifications of Defendant's failure to keep Plaintiff's and the Class's PII secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, date of birth, Social Security number, or driver's license number, without permission, to commit fraud or other crimes.

54. The types of PII compromised and potentially stolen in the Data Breach are highly valuable to identity thieves. The customers' stolen PII can be used to gain access to a variety of existing accounts and websites to drain assets, bank accounts or open phony credit cards.

55. Social Security numbers are particularly attractive targets for hackers because they can easily be used to perpetrate identity theft and other highly profitable types of fraud. Moreover,

Social Security numbers are difficult to replace, as victims are unable to obtain a new number until the damage is done.

56. Identity thieves can also use the stolen data to harm Plaintiff and Class members through embarrassment, blackmail, or harassment in person or online, or to commit other types of fraud including obtaining ID cards or driver's licenses, fraudulently obtaining tax returns and refunds, and obtaining government benefits. A Presidential Report on identity theft from 2008 states that:

In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health- related or criminal record fraud, face other types of harm and frustration.

In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.

57. As a result of MCS' failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

- a. The loss of the opportunity to control how their PII is used;
- b. The diminution in value of their PII;
- c. The compromise and continuing publication of their PII;
- d. Out-of-pocket costs associated with the prevention, detection, recovery, and

remediation from identity theft or fraud;

- e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;
- f. Delay in receipt of tax refund monies;
- g. Unauthorized use of stolen PII; and
- h. The continued risk to their PII, which remains in the possession of defendant and is subject to further breaches so long as defendant fails to undertake the appropriate measures to protect the PII in their possession.

58. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to \$1,000.00 depending on the type of information obtained.

59. The value of Plaintiff's and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

60. It can take victims years to spot identity or PII theft, giving criminals plenty of time to use that information for cash.

61. One such example of criminals using PII for profit is the development of "Fullz" packages.

62. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of

accuracy in order to assemble complete dossiers on individuals. These dossiers are known as “Fullz” packages.

63. The development of “Fullz” packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff’s and the proposed Class’s phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff’s and the Class’s stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

64. Defendant disclosed the PII of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and members of the proposed Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

65. Defendant’s use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, as evidenced by its complete failure to prevent malware in its systems, demonstrates a willful and conscious disregard for privacy, and has exposed the PII of Plaintiff and the Class to unscrupulous operators, con-artists, and criminals.

66. Defendant's failure to properly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff's and the Class's injuries by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

The Data Breach was a Foreseeable Risk of Which Defendant was on Notice.

67. It is well known that PII, including Social Security numbers, is an invaluable commodity and a frequent target of hackers.

68. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.⁹

69. In light of recent high profile data breaches, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), CMS knew or should have known that its electronic records would be targeted by cybercriminals.

70. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

71. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII private and secure, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

72. In the years immediately preceding the Data Breach, Defendant knew or should

⁹ Data breaches break record in 2021, CNET (Jan. 24, 2022), <https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/> (last visited March 6, 2024).

have known that Defendant's computer systems were a target for cybersecurity attacks, including ransomware attacks involving data theft, because warnings were readily available and accessible via the internet.

73. In October 2019, the Federal Bureau of Investigation published online an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector."¹⁰

74. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."¹¹

75. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."¹²

76. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that (i) ransomware actors were targeting entities

¹⁰ High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations, FBI, available at <https://www.ic3.gov/Media/Y2019/PSA191002> (last visited March 6, 2024).

¹¹ Ransomware mentioned in 1,000+ SEC filings over the past year, ZDNet, <https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/> (last visited March 6, 2024).

¹² Ransomware Guide, U.S. CISA, <https://www.cisa.gov/stopransomware/ransomware-guide> (last visited March 6, 2024).

such as Defendant, (ii) ransomware gangs were ferociously aggressive in their pursuit of entities such as Defendant, (iii) ransomware gangs were leaking corporate information on dark web portals, and (iv) ransomware tactics included threatening to release stolen data.

77. In light of the information readily available and accessible on the internet before the Data Breach, Defendant, having elected to store the unencrypted PII of thousands of its current and former customers and employees in an Internet-accessible environment, had reason to be on guard for the exfiltration of the PII and Defendant's type of business had cause to be particularly on guard against such an attack.

78. Before the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiff's and Class Members' PII could be accessed, exfiltrated, and published as the result of a cyberattack. Notably, data breaches are prevalent in today's society therefore making the risk of experiencing a data breach entirely foreseeable to Defendant.

79. Prior to the Data Breach, Defendant knew or should have known that it should have encrypted its customers' and employees' PII to protect against their publication and misuse in the event of a cyberattack.

Defendant failed to adhere to FTC guidelines.

80. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

81. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

- a. protect the personal customer information that they keep;
- b. properly dispose of personal information that is no longer needed;
- c. encrypt information stored on computer networks;
- d. understand their network's vulnerabilities; and
- e. implement policies to correct security problems.

82. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

83. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

84. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

85. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to former and current customers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

86. Several best practices have been identified that—at a minimum—should be

implemented by businesses like Defendant. These industry standards include: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

87. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

88. Upon information and belief Defendant failed to meet the minimum standards of one or more of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

89. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

CLASS ACTION ALLEGATIONS

90. Plaintiff sues on behalf of himself and the proposed Class ("Class"), defined as follows:

All individuals in the United States whose PII was accessed without authorization in the Data Breach, including all those who received a notice of the Data Breach.

91. Excluded from the Class is Defendant, its agents, affiliates, parents, subsidiaries,

any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

92. Plaintiff reserves the right to amend the class definition.

93. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

94. **Numerosity**. Plaintiff is representative of the proposed Class, consisting of more than a thousand members, far too many to join in a single action;

95. **Ascertainability**. Class members are readily identifiable from information in Defendant's possession, custody, and control;

96. **Typicality**. Plaintiff's claims are typical of Class member's claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

97. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. His interests do not conflict with Class members' interests, and he has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

98. **Commonality**. Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for all Class members. Indeed, it will be necessary to answer the following questions:

- a. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII;

- b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- c. Whether Defendant was negligent in maintaining, protecting, and securing PII;
- d. Whether Defendant breached contract promises to safeguard Plaintiff and the Class's PII;
- e. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;
- f. Whether Defendant's Breach Notice was reasonable;
- g. Whether the Data Breach caused Plaintiff's and the Class's injuries;
- h. What the proper damages measure is; and
- i. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

99. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

100. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

101. Plaintiff and members of the Class entrusted their PII to MC. Defendant owed a duty to Plaintiff and the Class to exercise reasonable care in safeguarding and protecting their PII and keeping it from being compromised, lost, stolen, misused, and or/disclosed to unauthorized

parties. This duty included, among other things, designing, maintaining, and testing Defendant's security systems to ensure the PII of Plaintiff and the Class was adequately secured and protected, including using encryption technologies. Defendant further had a duty to implement processes that would detect a breach of its security system in a timely manner.

102. MCS was under a basic duty to act with reasonable care when it undertook to collect, create, and store Plaintiff's and the Class's PII on its computer system, fully aware—as any reasonable entity of its size would be—of the prevalence of data breaches and the resulting harm such a breach would cause. The recognition of Defendant's duty to act reasonably in this context is consistent with, *inter alia*, the Restatement (Second) of Torts § 302B (1965), which recounts a basic principle: an act or omission may be negligent if the actor realizes or should realize it involves an unreasonable risk of harm to another, even if the harm occurs through the criminal acts of a third party.

103. Defendant knew that the PII of Plaintiff and the Class was information that is valuable to identity thieves and other criminals. Defendant also knew of the serious harms that could happen if the PII of Plaintiff and the Class was wrongfully disclosed.

104. By being entrusted by Plaintiff and the Class to safeguard their PII, Defendant had a special relationship with Plaintiff and the Class. Plaintiff's and the Class's PII was provided to MCS with the understanding that Defendant would take appropriate measures to protect it and would inform Plaintiff and the Class of any security concerns that might call for action by Plaintiff and the Class.

105. Defendant breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' PII by failing to adopt, implement, and maintain adequate security measures to safeguard that information and allowing unauthorized access to

Plaintiff's and the Class's PII.

106. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and the Class, their PII would not have been compromised, stolen, and viewed by unauthorized persons. Defendant's negligence was a direct and legal cause of the theft of the PII of Plaintiff and the Class and all resulting damages.

107. The injury and harm suffered by Plaintiff and the Class members was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' PII.

108. As a result of Defendant's failure, the PII of Plaintiff and the Class were compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their PII was disclosed to third parties without their consent. Plaintiff and Class members also suffered diminution in value of their PII in that it is now easily available to hackers on the Dark Web. Plaintiff and the Class have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

109. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

110. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and members of the Class's PII.

111. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as

Defendant, of failing to use reasonable measures to protect consumers' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the Class's sensitive PII.

112. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

113. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

114. Defendant had a duty to Plaintiff and the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and the Class's PII.

115. Defendant breached its respective duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and members of the Class's PII.

116. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

117. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and members of the Class, Plaintiff and the Class would not have been injured.

118. The injury and harm suffered by Plaintiff and the Class were the reasonably

foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

119. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

COUNT III
Intrusion upon Seclusion/Invasion of Privacy
(On Behalf of Plaintiff and the Class)

120. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

121. The State of Texas recognizes the tort of Intrusion upon Seclusion, and adopts the formulation of that tort found in the Restatement (Second) of Torts, which states:

One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Restatement (Second) of Torts § 652B (1977).

122. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

123. Defendant owed a duty to its current and former employees and customers, including Plaintiff and the Class, to keep this information confidential.

124. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff's and Class

members' PII is highly offensive to a reasonable person.

125. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

126. The Data Breach constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

127. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

128. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

129. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

130. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages (as detailed *supra*).

131. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII are still maintained by Defendant with their inadequate cybersecurity system and policies.

132. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiff and the Class.

133. In addition to injunctive relief, Plaintiff, on behalf of themselves and the other Class members, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

COUNT IV
Breach of Implied Contract
(On behalf of Plaintiff and the Class)

134. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

135. Plaintiff and Class Members were required to provide their PII to Defendant as a condition of receiving employment and/or services from Defendant. Plaintiff and Class Members provided their PII to Defendant in exchange for employment and/or services with Defendant.

136. Plaintiff and the Class Members accepted Defendant's offers by disclosing their PII to Defendant in exchange for employment and/or its services.

137. In turn, and through internal policies, Defendant agreed to protect and not disclose the PII to unauthorized persons.

138. In its Privacy Policy, Defendant represented that it "employs technical safeguards, as well as internal policies, procedures, and controls, to protect the information from unauthorized access or disclosure."¹³

139. Implicit in the parties' agreement was that Defendant would provide Plaintiff and

¹³ Privacy Policy, MCS, <https://mcs360.com/privacy-policy/> (last visited March 6, 2024).

Class Members with prompt and adequate notice of all unauthorized access and/or theft of their PII.

140. After all, Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of such an agreement with Defendant.

141. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

142. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

143. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

144. Defendant materially breached the contracts it entered with Plaintiff and Class Members by:

- a. failing to safeguard their information;
- b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.
- c. failing to comply with industry standards;
- d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

- e. failing to ensure the confidentiality and integrity of the electronic PII that Defendant created, received, maintained, and transmitted.

145. In these and other ways, Defendant violated its duty of good faith and fair dealing.

146. Defendant's material breaches were the direct and proximate cause of Plaintiff's and Class Members' injuries (as detailed *supra*).

147. Plaintiff and Class Members performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

COUNT V
Unjust Enrichment
(On behalf of Plaintiff and the Classes)

148. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

149. This claim is pleaded in the alternative to the breach of implied contract claim.

150. Plaintiff and Class members conferred a benefit upon Defendant. After all, Defendant benefitted from using their PII to facilitate employment, its provision of services, and its collection of payment.

151. Defendant appreciated or had knowledge of the benefits it received from Plaintiff and Class members. And Defendant benefited from receiving Plaintiff's and Class members' PII, as this was used to facilitate employment, its provision of services, and its collection of payment.

152. Plaintiff and Class members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

153. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class members' PII.

154. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations

at the expense of Plaintiff and Class members by utilizing cheaper, ineffective security measures. Plaintiff and Class members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

155. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and Class members' payment because Defendant failed to adequately protect their PII.

156. Plaintiff and Class members have no adequate remedy at law.

157. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiff and Class members—all unlawful or inequitable proceeds that it received because of its misconduct.

COUNT VI
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

158. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

159. Given the relationship between Defendant and Plaintiff and Class members, where Defendant became guardian of Plaintiff's and Class members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for Plaintiff and Class members, (1) for the safeguarding of Plaintiff's and Class members' PII; (2) to timely notify Plaintiff and Class members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

160. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of Defendant's relationship with them—especially to secure their PII.

161. Because of the highly sensitive nature of the PII, Plaintiff and Class members would

not have entrusted Defendant, or anyone in Defendant's position, to retain their PII had they known the reality of Defendant's inadequate data security practices.

162. Defendant breached its fiduciary duties to Plaintiff and Class members by failing to sufficiently encrypt or otherwise protect Plaintiff's and Class members' PII.

163. Defendant also breached its fiduciary duties to Plaintiff and Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

164. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

COUNT VII
Breach of Confidence
(On Behalf of Plaintiff and the Class)

165. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

166. At all times during Plaintiff's and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' PII that Plaintiff and Class Members were provided to Defendant in exchange for its services.

167. As alleged herein and above, Defendant's relationship with Plaintiff and Class Members was governed by expectations that Plaintiff's and Class Members' PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

168. Plaintiff and Class Members provided their respective PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII to be disseminated to any unauthorized parties.

169. Plaintiff and Class Members also provided their respective PII to Defendant with the explicit and implicit understanding that Defendant would take precautions to protect that PII from unauthorized disclosure, such as following basic principles of information security practices.

170. Defendant voluntarily received in confidence Plaintiff's and Class Members' PII with the understanding that the PII would not be disclosed or disseminated to the public or any unauthorized third parties.

171. Due to Defendant's failure to prevent, detect, and/or avoid the data breach from occurring by, inter alia, failing to follow best information security practices to secure Plaintiff's and Class Members' PII, Plaintiff's and Class Members' PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

172. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class Members have suffered damages.

173. But for Defendant's disclosure of Plaintiff's and Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data breach was the direct and legal cause of the theft of Plaintiff's and Class Members' PII, as well as the resulting damages.

174. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' PII. Defendant knew its computer systems and technologies for accepting and securing Plaintiff's and Class Members' PII had numerous security vulnerabilities because Defendant failed to observe industry standard information security practices.

175. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff

and the Class have suffered, and continue to suffer, injuries and damages arising from identity theft; damages from lost time and effort to mitigate the actual and potential impact of the data breach on their lives, including, inter alia, contacting their financial institutions, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, signing up for credit monitoring, and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

176. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

PRAYER FOR RELIEF

177. Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

- A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing his counsel to represent the Class;
- B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;
- C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff

and the Class;

- D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;
- E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;
- F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;
- G. Awarding attorneys' fees and costs, as allowed by law;
- H. Awarding prejudgment and post-judgment interest, as provided by law;
- I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and
- J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

DATED: March 14, 2024

Respectfully submitted,

/s/ Joe Kendall

Joe Kendall
Texas Bar No. 11260700
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 825
Dallas, Texas 75219
Telephone: 214/744-3000 / 214/744-3015 (fax)
jkendall@kendalllawgroup.com

Samuel J. Strauss*
sam@turkestrauss.com
Raina C. Borrelli *
raina@turkestrauss.com
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, WI 53703
Telephone (608) 237-1775
Facsimile: (608) 509-4423

Attorneys for Plaintiff

**Pro Hac Vice Forthcoming*